СЛЕДСТВИЯ ИЗ МАЛОЙ ТЕОРЕМЫ ФЕРМА

КОРНИ МНОГОЧЛЕНА $x^{p-1}-1$ НАД $\mathbb{Z}/p\mathbb{Z}$

Так как по малой теореме Ферма $1^{p-1}, 2^{p-1}, \ldots, (p-1)^{p-1}$ сравнимы с 1 по модулю p, то многочлен $x^{p-1}-1$ имеет ровно $p-1$ различный корень над $\mathbb{Z}/p\mathbb{Z}$ (все ненулевые остатки — его корни).

А следовательно, имеет место разложение:

$x^{p-1}-1 \equiv (x-1)(x-2)\ldots(x-p+1) \bmod p$.

Например, $p = 2017$. Тогда выполнено:

$(x-1)(x-2)\ldots(x-2016) \equiv (x^{2016}-1) \bmod 2017$,

т.е. при перемножении все остальные слагаемые оказываются кратными 2017.

Проверим истинность этого утверждения при $p = 5$. Рассмотрим произведение $(x-1)(x-2)(x-3)(x-4)$ по модулю 5. Имеем:

$(x-1)(x-2)(x-3)(x-4) = (x^2-3x+2)(x^2-7x+12) =$
$= x^4+(-3-7)x^3+(12+2+21)x^2+(-2\cdot 7-12\cdot 3)x+24 =$
$= x^4-10x^3+35x^2-50x+24 \equiv x^4-1 \bmod 5$,

что и требовалось установить.

УПРАЖНЕНИЕ

Проверить для $p = 7$, применяя деление с остатком x^6-1 на $x-1$, $x-2$ и т.д. Убедиться, что каждый раз деление будет без остатка.

Из полученного разложения мы получим несколько удивительных и очень красивых результатов.

ТЕОРЕМА ВИЛЬСОНА

Мы уже доказали теорему Вильсона на одном из предыдущих уроков. Теперь мы ее выведем из МТФ.

ТЕОРЕМА ВИЛЬСОНА

Для любого простого нечетного p
$(p-1)! + 1$ делится на p.

ДОКАЗАТЕЛЬСТВО

В самом деле, рассмотрим основное полиномиальное тождество по модулю p:
$x^{p-1}-1 \equiv (x-1)(x-2)\ldots(x-p+1) \bmod p$.

Отсюда следует, что коэффициенты при каждой степени x слева и справа сравнимы по модулю p.
В частности, сравнимы и свободные члены:
$-1 \equiv (-1)(-2)\ldots(-(p-1)) \bmod p$.

При нечетном p количество «минусов» в произведении справа будет четным. Тогда:
$-1 \equiv (p-1)! \bmod p$. Что и требовалось доказать.

Вспомним основное утверждение в рождественской теореме Ферма.

УТВЕРЖДЕНИЕ

$-1 \equiv c^2 \bmod p \quad \Leftrightarrow \quad p = 4k+1$.

Ранее мы доказали это утверждение только в одну сторону, а теперь докажем полностью.

Проведем подготовительную работу.
Рассмотрим $1^2, 2^2, \dots (p-1)^2$ по модулю p.

Вопрос: Сколько среди них различных? Не более, чем $\frac{p-1}{2}$:

$p - 1 \equiv -1 \bmod p \Rightarrow 1^2 \equiv (-1)^2 \equiv (p-1)^2 \bmod p$;
$p - 2 \equiv -2 \bmod p \Rightarrow 2^2 \equiv (-2)^2 \equiv (p-2)^2 \bmod p$ и т.д.

Далее мы докажем, что различных квадратов ровно $\frac{p-1}{2}$, то есть половина остатков является квадратами, а половина — нет.

Остатки, которые являются квадратами других остатков по некоторому модулю, называются **квадратичными вычетами**, а которые не являются квадратами — **квадратичными невычетами**.

КОЛИЧЕСТВО КВАДРАТИЧНЫХ ВЫЧЕТОВ ПО МОДУЛЮ p

Пусть $p = 11$. Перечислим все квадраты остатков по модулю p:
$1^2 = 1, 2^2 = 4, 3^2 = 9, 4^2 = 16 \equiv 5, 5^2 = 25 \equiv 3,$
$6^2 = 36 \equiv 3, 7^2 = 49 \equiv 5, 8^2 = 64 \equiv 9, 9^2 \equiv 4, 10^2 \equiv 1$.

Получили 5 различных квадратичных вычетов: 1, 4, 9, 5, 3.

Докажем, что при любом p их ровно $\frac{p-1}{2}$.

От противного. Пусть существует повтор:
$c = a^2 \equiv b^2 \equiv (-a)^2 \equiv (-b)^2 \bmod p$.

Тогда многочлен $x^2 - c$ имеет минимум 4 корня по модулю p.
Получили противоречие.

Из этого в частности следует, что все квадраты первой половины остатков будут различны, а остальные будут их повторять.

ДОКАЗАТЕЛЬСТВО УТВЕРЖДЕНИЯ ИЗ РТФ

Теперь рассмотрим многочлен $x^{\frac{p-1}{2}} - 1$. Все квадратичные вычеты являются его корнями по малой теореме Ферма. Следовательно, других корней у этого многочлена нет.

Итак, имеем разложение:

$$x^{\frac{p-1}{2}} - 1 \equiv (x - 1^2)(x - 2^2) \dots \left(x - \left(\frac{p-1}{2}\right)^2\right) \bmod p.$$

Отсюда a — квадратичный вычет $\Leftrightarrow a^{\frac{p-1}{2}} \equiv 1 \bmod p$;

a — квадратичный невычет $\Leftrightarrow a^{\frac{p-1}{2}} \equiv -1 \bmod p$, т.к.

$x^{p-1} - 1 = \left(x^{\frac{p-1}{2}} - 1\right)\left(x^{\frac{p-1}{2}} + 1\right)$, и половина остатков являются корнями первого многочлена, а другая половина — корнями второго.

Вернемся к утверждению из РТФ, которое мы хотим доказать.

Получаем:

$a = -1$ — квадратичный вычет по модулю

$p \Leftrightarrow (-1)^{\frac{p-1}{2}} \equiv \bmod p \Leftrightarrow \frac{p-1}{2}$ — четно, т. е. $\frac{p-1}{2} = 2k \Leftrightarrow$

$p = 4k + 1$ для некоторого целого k. Ч. т. д.

Это рассуждение служит точкой в доказательстве РТФ и одновременно началом для новых очень интересных результатов.

На следующих уроках мы докажем существование первообразного корня для любого простого модуля, а также сформулируем квадратичный закон взаимности Гаусса.